# Facing the Post-Cold War Era



*The world has moved into a new era. NSA, as a product of an earlier age and its circumstances, must adjust to the realities of the late twentieth century.*

*Three circumstances fundamental to the creation of the post-1945 American national security community have undergone dramatic revision in recent years. The end of the cold war is the most dramatic of the fundamental changes that will affect NSA's future, but a radical transformation of information technology may be even more basic in its impact and contributed significantly to the collapse of the Soviet Union. Finally, the American political climate toward intelligence has changed, largely because of changes in the threat and information environments.*

## CONCEIVED IN CRISIS: THE WARTIME ENVIRONMENT

The modern American national security community, the overall defense, foreign policy, and intelligence efforts of the United States government are the product of wartime conflicts against totalitarian regimes. Only the first few years of the period 1941–1991 involved direct conflict with a principal adversary, and the country even entertained a brief moment (1945–1948) when it was possible to at least hope, as the U.S. had after 1918, for a return to normalcy. Throughout most of the period, however, the United States behaved as if it were a country engaged in a struggle for national survival.

Beginning in the late 1930s, the United States began to expand its capacity to deal with an increasingly troubled world situation. Consistent with American tradition, this peacetime expansion in the face of possible military action developed cautiously and in the face of considerable domestic political opposition.

Though most of that opposition focused on the more overt forms of military expansion, including increased budgets and the passage of a national service act, a deep suspicion of intelligence operations was also part of American tradition. The country that believed in "open covenants openly arrived at" and "gentlemen do not read each other's mail" also feared the potential abuse of government power, especially power exercised in secret.

The debate over increased defense expenditure, which was really a debate over America's role in world affairs, was not resolved by political debate or a change in American values. It was of course resolved by the Japanese attack on Pearl Harbor. The United States then undertook the extraordinary (in every sense of the word) exertions that culminated in the Allied victory over Germany and Japan.

Contrary perhaps to the popular view of the period after 1945, however, the Second World War did not produce a dramatic renunciation of the attitudes prevalent in American culture after the First World War. Warren Harding may have promised a return to "normalcy"; Harry Truman, for the first year or so of his administration, promised a return to "economy and efficiency" and the most rapid demobilization possible. Well into 1946 and 1947, the prospects for a large peacetime military establishment were as poor as they had been in 1920. The prospects for a significant peacetime intelligence establishment were even lower. Lacking the permanent, traditional bureaucratic establishment of the military services, recognized in two cabinet positions, the intelligence apparatus of the wartime era simply went away. The Office of Strategic Services was disbanded, and those remnants of its operations that were not eliminated were returned to control of the military departments or to the State Department. On the cryptologic side, prospects looked scarcely more promising.

What, then, led the American people to reverse course and support the establishment of a large, expensive peacetime military security establishment? It took little short of a heroic effort by Truman, Secretary of State George Marshall, and a bipartisan congressional leadership to convince the American people that their country was really at peace.

By 1948, it was clear to men like Truman and Marshall that the American people must be asked to make an unprecedented peacetime commitment not only to the defense of the United States and its direct interest but to the defense of major areas of the world. The only way to justify that commitment was to define the threat from the Soviet Union and its clients as virtual war. Through four decades and nine presidencies, the United States took on a burden as extensive as it was complex: defending itself and its World War II allies, assisting in the reconstruction of formerly occupied Europe, and even not just rebuilding the economies of our former adversaries but implanting – successfully – democratic political structures.

A global war, cold or not, required a global system of bases, security arrangements, and intelligence requirements. More importantly, it demanded that intelligence operate on a stringent wartime understanding of both the value of security, especially the restriction of access to information, and the potential cost of security breaches.

Almost inevitably, the creation of a robust national security establishment in a period of formal peace but potentially devastating conflict raised significant issues involving fundamental American values and principles. In times of crisis, societies move to defend themselves by methods that would be neither required nor tolerated in more tranquil periods. For most of the cold war, for example, the American people accepted conscription, something we had never done in peacetime except in the period immediately preceding World War II. (And, of course, even that aberration, initiated in 1940, survived by a single vote in the Congress as late as November 1941.) Over the last decade, the threat of terrorism has forced travelers to accept as normal restrictions on their activities and infringements of their privacy that even a generation before would have been technically impossible and morally intolerable. But "tolerable" is not "normal," nor does it equate to

"desirable." Deviations from preferred practice are not likely to survive the demise of the conditions that led to the deviation in the first place.

The United States has conducted secret operations throughout its history, but these have always been limited in scope and viewed with great alarm by Americans who feared the possible misuse of secret police and intelligence powers. Even in the immediate post-World War II period, it was the traditional opponents of American involvement overseas, largely midwestern conservatives like Robert Taft of Ohio, who expressed some of the sharpest skepticism about the dangers of an expanded national security system. Such a system, Taft argued, would cost enormous amounts of money, far more than its advocates were prepared to admit, and would of necessity result in inevitable expansions of government power and at least occasional, if not systematic, abuses of that power.

Ultimately, the realities of the post-1945 era required the concessions Taft and others warned about. Truman and his associates were able to win the case that the United States was at war. Alarmed by the generally thuggish behavior of the Stalinist Soviet Union, the American people, led by a bipartisan political leadership, took on the responsibilities of being a world power. Moreover, it can be argued that this effort produced significant permanent change in American attitudes toward international affairs. It would be a mistake, nevertheless, to assume that the American people have experienced a fundamental shift away from a reluctance to see large military (and intelligence) establishments as a permanent feature of their lives. That cause has hardly been made, let alone accepted.

NSA was born in the first surge of the American commitment to the long and difficult struggle against Soviet communism. Its founders were the men and women who had built the successful American cryptologic effort against Germany and Japan. Their challenge was to build and operate a cryptologic system to be directed against an adversary that represented a mortal threat to the survival of the United States. Over time, with the collapse of the European empires in Asia and Africa, the fall of Nationalist China, and the Soviet Union's endorsement of wars of national liberation, the SIGINT effort – like the rest of the national security effort – became global. Even in the case of countries of little or no intrinsic value or interest to the United States – and there are many of them – the globalized contest between the United States and the Soviet Union led the U.S. to do a crash course in the language and cultures (and communications systems) of countries it had traditionally ignored. When Winston Churchill was once confronted by an aide noting events taking place in some obscure country, Churchill is said to have remarked that it was his habit not to bother with such states as long as they did not bother him. After 1945, almost no countries fell below the threshold of American interest.

## THE TOTALITARIAN ADVERSARY

The presence of a credible adversary was necessary to obtain a popular commitment to support large defense expenditures in the post–1945 era. The nature of that adversary

determined the role and structure of the intelligence component of America's cold war security apparatus.

The peculiar heresy of the twentieth century, totalitarianism represents the subordination of the institutions of society to state control. Its chosen instruments were violence intentionally applied to intimidate or eliminate real or potential opposition and control of information to reduce the prospect of opposition.

The efforts of the totalitarian states to control information opened a new chapter in the history of intelligence. Nazi Germany, the Soviet Union, and their imitators not only restricted access to information but made unprecedented efforts to produce disinformation. Keep in mind that only a generation or two before, the shipyards and arsenals of the great powers were opened to foreign observers except during times of war and that the practice of allowing neutral armies to station observers with the armies of belligerents continued into the First World War. Restrictions on the press were limited or nonexistent. (In some armies, serving officers even added to their pay by acting as special correspondents for newspapers. This may have been frowned upon, but one suspects more on the grounds of social propriety than security.)

The totalitarian challenge put open-source information media at great disadvantage in both timeliness and access. Even more importantly, the skilled manipulation of information by the totalitarian states put open sources under even greater handicap. Goering's ability to impress Charles Lindbergh with the power of the prewar Luftwaffe, the success of Theresienstadt in averting criticism of Germany's treatment of Europe's Jews, and Soviet use of May Day flyovers to give an exaggerated impression of the size of the Soviet bomber fleet are but examples of the success the totalitarians achieved in corrupting information. Czarist Russia may have invented the Potemkin village, but by the standards of the twentieth century the old authoritarian states were mere amateurs at disinformation.

In these circumstances, the process of obtaining information from covert or clandestine sources received the highest priority. This was not a world in which the democracies could be fastidious about collection methods or about retaining the older, more civil order. Still they tried. The Open Skies proposal advanced by the United States was an effort to retain something of the civility of an older world in which most information was not protected from outside view. The failure of such efforts, combined with a critical need for information on the Soviet Union, led the U.S. to undertake extraordinary collection efforts, including the U-2 program.

## THE NEW WORLD INFORMATION ORDER

A combination of changed geopolitical circumstances and more effective information technology has altered the balance between open-source and restricted information. In both availability and value, the balance has shifted in the direction of – though not fully in favor of – open-source information. Moreover, this process is likely to continue, effectively

devaluing efforts at information restriction. More and more of the information that counts in the world, information that can be acted on by decision makers, is available for public acquisition. This does not mean that open source is the only information of value; it does mean that the collectors and suppliers of restricted information need to emphasize information that cannot be obtained by open means. At some level, we have always understood this, but our operating environment has not always put us under pressure to act on this understanding. As the layering study put it, NSA has carried out its mission "effectively but not efficiently." In the new information order, we will be forced to pay far more attention to efficiency, not only because we will have fewer resources to waste but because our overseers will be far more critical in assessing the costs versus benefits of open versus classified information.

We are not the only collection source that will feel increased competition. The advent of satellite imagery was a major (but expensive) breakthrough for the U.S., providing it with a window over the wall erected by the Soviet Union and other closed societies. Now, less than a generation later, the same basic technology that was once one of America's most closely guarded secrets not only is universally known but is increasingly available on a commercial basis. In this as in most other aspects of technology, that which in one generation was esoteric becomes, a generation or so removed, commonplace.

Even more dramatic is the increased access of open-source media, often equipped with their own satellite communication equipment. The days of the war correspondent armed with notepad, pencil, and possibly camera look quaint in an age when CNN seems to provide everything from live coverage of the 1991 coup attempt in the Soviet Union to forward air observation on the first night of DESERT STORM. What would Goebbels say?

As late as the 1970s, information technology made systematic restrictions on information seem at least feasible. Even in the 1980s, some third world states, led by India, even thought it possible to restrict information flow across borders the way governments control civil aviation. Only a short time later, in an age of global CNNization, this idea has a quaintly antiquarian quality to it. Within a few decades, resistance movements in the Soviet Union went from laborious republication of banned texts using manual typewriters and carbon paper (only a true friend of liberty would attempt to retype a Russian novel) to more humane and efficient duplication on floppy disks. Not surprisingly, the Soviet Union information regime and the political regime on which it depended could neither suppress nor survive this development.

The greatest impact of the new world information order has been felt on those regimes that most attempted to control information. Its impact is nonetheless felt on the democracies, which in their own ways attempted, in most cases with restraint, to control information that might aid their adversaries. As Churchill noted, in critical times, truth itself must sometimes be "protected by a bodyguard of lies."

One can argue with Churchill's moral pragmatism, but the fact remains that if the industrial democracies stepped reluctantly into information control; propaganda, and even disinformation, their adversaries fairly wallowed in them. For the totalitarian states,

control of information from their adversaries was probably at all times of secondary importance to their need to control the flow of information to their own people. In the democracies, information controls no doubt proved useful in limiting or controlling the access of information to the peoples of those democracies, but such abuses tended to be marginal and subject to challenge by a deeply embedded sense of the supremacy of the public's right to know over the government's right to regulate information. Only in retrospect will we be able to judge the success the democracies enjoyed in this delicate balancing act, but the short-term view must be that both sides – those struggling to control essential information and those pressing for limits on such controls – performed functions in a generally responsible manner. As Macauley noted, ships require sails and anchors alike.

The question now for the democracies is how they will deal with information security standards in a world in which the great enemy has disappeared and the technology of information dissemination appears to have the advantage over the technology of information control. Which of our many traditional practices in clearances, compartmentation, and so on make moral and political sense in the new environment? Which are even technically feasible? At what point does ease of access assume greater importance than guaranteed security? Given the reduced external threat, is more information simply harmless if released?

It is perhaps a compliment to the American character that even among the industrial democracies we were the most embarrassed and uncomfortable with restrictions on freedom of information as well as on the other moral and in some cases legal concessions we made to necessity. Americans have never been as comfortable as the French, for example, in rationalizing questionable actions as consistent with raison d'etat. President Eisenhower was greatly embarrassed by the discovery of U-2 flights over the Soviet Union, even more by having to back down from a public "misstatement" on the topic. Most cold war presidents suffered similar embarrassments in one form or another, as incident after incident gradually revealed the degree to which the United States government had been forced to make concessions to the realities of living in a world constantly at risk of annihilation. Even in the period after large-scale disclosure and increased congressional oversight, the American people demonstrated a willingness to approve, however grudgingly, modifications to some of our older, more traditional views of correct interstate behavior. We should not underestimate, however, the cost we have paid for this change, especially in public trust in government.

## THREAT ASSESSMENT AND PUBLIC TOLERANCE IN THE POST-COLD WAR WORLD

While the passing of the wartime environment of the historic conflict between the industrial democracies and the totalitarian states, public support in the democracies for wartime measures in both military expenditure and other forms of national security activity will wane. The United States and its allies have already cut defense budgets significantly, and additional cuts are likely, barring the rise of some unforeseen threat. In

mentioning the prospect of such a threat, we should not consider such issues as the possibility of a military takeover of Russia, continued fighting in the Balkans, or nth country proliferation. The American public has heard of these, has factored them into its thinking, and to this point sees no connection between them and an effort to halt or reverse reduced expenditures.

Even the case of militarist, nuclear-armed Russia, for example, will not automatically lead to a reversal of the prevailing trends. The American people would demand argument and evidence that such a development directly threatened the United States before reacting to it. In the late 1940s, it was the president who was from Missouri; it was the American people who said "show me." A similar skepticism would apply to any new call to arms.

Intelligence will face an even deeper skepticism. Some months ago, in the first wave of realization that the collapse of communism would permit a reduction in American defense spending, a senior member of the House Armed Services Committee told a television interviewer that a second "peace dividend" existed in the form of the intelligence budget: "If you don't have any enemies, who is there to spy on?" Whatever one thinks of this view, it reflects a continuing American tendency to believe that intelligence is a necessary wartime task, not a permanent function of government in peace as well as war.

Skepticism will also confront efforts to maintain cold war standards of information security. Already, historians and others are campaigning for more rapid and systematic declassification of the records of the cold war. It is unseemly, the argument goes, for the world's greatest democracy to be withholding information while the heirs to the archives of the Soviet Union and its East European clients open theirs.

The argument can and should be made that going concerns do not operate under the same rules governing bankrupt ones. The United States still has interests that must be considered in declassification decisions. Strictly speaking, the Soviet Union et al. have no interests at all, and their successors may have only limited (but possibly crucial) interests in the records of the former regimes. It is legitimate to suggest to advocates of total declassification that the states of the former Soviet bloc may not be meeting the standard of totality themselves and that we have limited means to assess what is being held back.

Public and congressional support for restrictions on other forms of information access is likely to decline as well. The failure of the Reagan administration's efforts to create a "semi-classified" categorization for information not formally covered by existing classification systems ran afoul of both a technical climate that enhances dissemination over restriction and a culture increasingly uncomfortable with government restrictions.

In the cold war, security came close to being an absolute. At the very least, the argument for restrictions that promised the benefit of security had significant advantages over advancing the benefits of greater access. Times have changed. In fact, the public, through its elected representatives, is likely to be increasingly skeptical of claims of "national security" and less willing to grant infringements on personal liberty and freedom of information. It may be true, for example, that government-imposed or self-

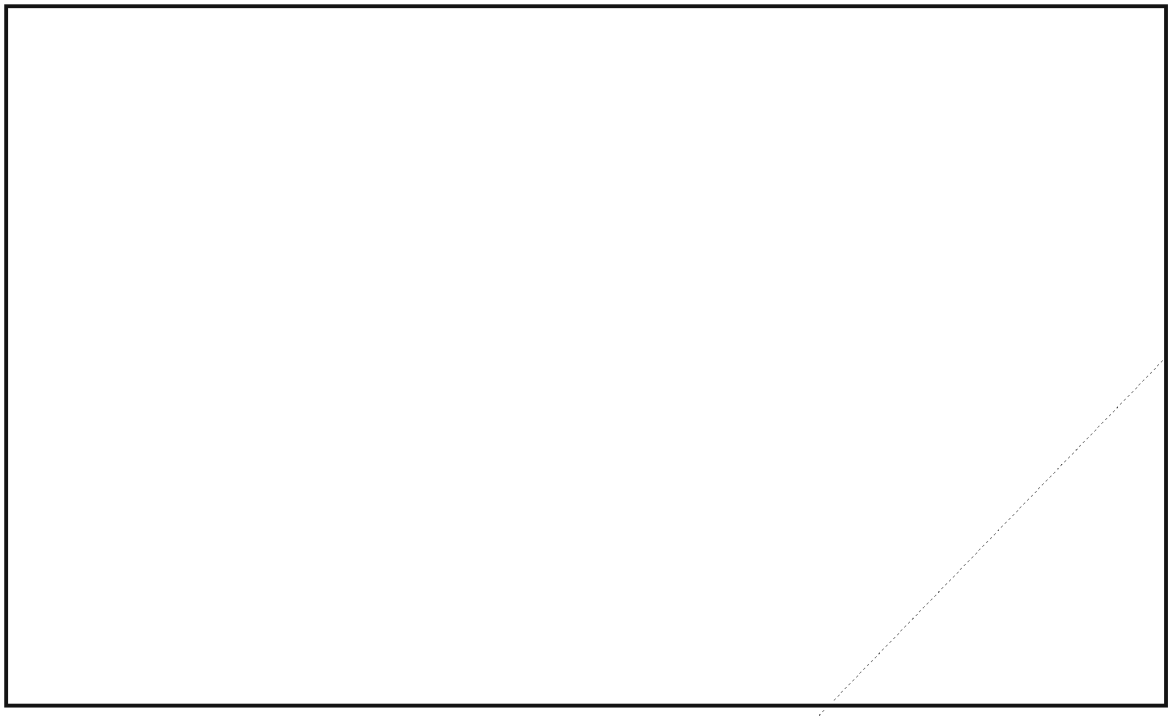
imposed restrictions on communications systems would enhance law enforcement's ability to convict major drug dealers. It may be, however, that the public is prepared to forego that edge in the interest of a more traditional sense of suspicion of overweening government power. We should anticipate similar reluctance to approve restriction on other forms of communications and information technology in the name of national security or the enhanced operations of the U.S. government. We should not be surprised when industry's claim that such restrictions hamper U.S. competitiveness seem to take on equal weight with congressional and executive policy makers. Nor should we be surprised when industry forms semi-unnatural alliances with advocacy groups to combine arguments on freedom of information grounds with the argument from competitiveness.

In short, we should not expect the wartime tolerance for secrecy and attendant restrictions to survive the transition to peacetime, assuming, of course, that we enter into a period more truly peaceful and less threatening than that which has confronted us over the last fifty years. For the present, at least, all signs suggest that we will at least move toward "normalcy," with the extent of that shift unforeseeable. We will probably not see all swords turned into ploughshares, but we will see a reduction of the resources society is prepared to put into swords. And for that, as citizens, we should all be grateful.

For NSA, survival in this new era first of all requires that we recognize its presence and attempt to assess its main characteristics. For the latter, the proverbial hardships of "painting a moving train" apply. We will need to be constantly engaged in monitoring environmental change.

We need to be prepared to deal with unpleasant or potentially unpleasant aspects of the new environment with imagination and discrimination. What changes will be merely unpleasant and which ones present vital threats? Moreover, we will need to be careful about defining those threats nationally and in terms of policy, not as institutional threats. In a policy sense, the president of the United States or Congress needs to protect the National Security Agency only when it clearly advances national policy. And we, along with other parts of the national security establishment, will increasingly see our arguments for or against policy change as reflecting self-interest rather than national interest, a reluctance on the part of the dinosaurs of the cold war to protect our appropriations.

We will need to conceive of the heretofore inconceivable. How should we respond to calls for rapid declassification of records with few, if any, exceptions? Are we prepared to deal with an international movement to consider the regulation of intelligence operations? Or a proposed international covenant protecting diplomatic communication from interception by third parties? In the post-cold war climate, our reaction to developments such as these will need to be something other than a reflexive development of the status quo. Our reaction will need to reflect a careful analysis of real costs, in terms meaningful to the policy maker. Most of all, we need to be prepared to face almost any challenge, even those that seem more appropriate to an era in which it could be thought, if not said, that gentlemen do not read one another's mail.



STATUTORILY EXEMPT